LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Privacy & Cyber Practice

May 20, 2024 | Number 3265

Riding the Wave: US Privacy Laws Continue to Proliferate in 2024

Businesses need to be proactive in updating their compliance measures to meet the ever-evolving set of privacy laws and regulatory expectations in 2024 and beyond.

Following the notable uptick in state-level privacy laws in 2023, a wave of new comprehensive state privacy laws and state laws seeking to regulate health privacy, youth privacy, online platforms, and data brokers are set to take effect this year. While a draft federal comprehensive privacy law — the American Privacy Rights Act — aimed at harmonizing this patchwork of state laws was introduced last month, until such a law actually passes, the quickly evolving state regulatory landscape will continue to set the standards for how most businesses must handle personal information in the US.

The state privacy laws taking effect this year introduce a variety of new obligations for businesses, especially those that process common forms of so-called "sensitive" personal information.

New Comprehensive State Privacy Laws

By the end of 2023, comprehensive privacy laws were in effect in five states: California, Colorado, Connecticut, Utah, and Virginia. In 2024, the laws of Texas, Florida, Oregon, and Montana will join the patchwork, increasing compliance obligations for businesses that process consumers' personal information in these states. Looking beyond 2024, comprehensive state privacy laws will also come into force in Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, and Maryland in 2025, and Indiana and Kentucky in 2026. And many similar laws are making their way through other state legislative bodies.

Laws Taking Effect in 2024

On July 1, 2024, most provisions of the Texas Data Privacy & Security Act (TDPSA / HB 4), Oregon Consumer Privacy Act (SB 619), and Florida Digital Bill of Rights law (FDBR / SB 262) will become operative. While these regulations share many similarities with the state laws already in effect, they each carve their own path in certain respects, including in their scope of application and specific compliance requirements. For instance, while the Texas law is largely modeled after the Virginia law, it will reach out-of-state companies with products or services merely "consumed by" Texas residents, as opposed to the Virginia law and most other comprehensive state privacy laws, which apply only to companies that "target" their products or services to in-state residents.

Similarly, although the Oregon law mirrors the Colorado law in many respects, it does not follow the Colorado law or most other comprehensive state privacy laws in exempting all institutions and affiliates that are subject to the federal Gramm-Leach-Bliley Act (GLBA). Instead, the Oregon law only exempts "financial institutions" as the term is defined under the Oregon Bank Act, which is narrower than the definition under the GLBA. As a result, the Oregon law in effect only exempts traditional banks and credit unions, leaving businesses that provide other consumer financial products or services in scope.

In Florida, aside from certain universal requirements that apply to all for-profit businesses doing business in Florida that sell sensitive information about Florida residents, the law will likely only affect certain large, enterprise companies due to its high annual revenue threshold and other applicability limitations. For such enterprise companies, the law affords unique rights to opt out of (i) the collection or processing of information about a known minor under the age of 18, (ii) the collection of personal information through voice or facial recognition features, and (iii) targeted advertising based on personal data obtained from the individual's activities across both unaffiliated *and affiliated* websites and online applications (see more on Texas, Oregon, and Florida).

Lastly, Montana's Consumer Data Privacy Act (SB 384), influenced by both the Virginia and Connecticut laws, will take effect this year on October 1 (see more on this law here). In line with requirements under the Connecticut law and certain other state comprehensive privacy laws (but not the Virginia law), the Montana law mandates that businesses recognize consumers' choice to opt out of the sale of their personal information and the processing of their personal information for purposes of targeted advertising submitted through an "opt-out preference signal" by January 1, 2025.

New State Consumer Health Privacy Laws and Increased Regulatory Focus on Health and Other Sensitive Information

As state and federal regulators focus their attention increasingly on businesses' use of sensitive information, in particular health-related information, three new landmark state health privacy laws are now in effect in Washington, Nevada, and California. These laws impose significant obligations that go beyond any prior laws governing health data, sweeping in many companies that likely do not consider their businesses to be particularly healthcare-focused.

Washington's My Health My Data Act (MHMD / HB 1155) and the Nevada Health Data Privacy Law (SB 370) both took effect on March 31, 2024 (with some exceptions, here). These laws regulate the use of "consumer health data," defined broadly as personal information that can be used to identify a consumer's physical or mental health condition or diagnosis. Because they apply to health information outside the scope of the Health Insurance Portability and Accountability Act, the laws potentially impose obligations on a large swath of businesses that sit outside the healthcare industry.

For example, the laws cover precise location information that could suggest an individual's attempt to receive health services, or data that is originally unrelated to health, but can be linked to health data through machine learning or algorithms. Under these laws, covered companies both inside and outside of the healthcare industry must implement specific compliance measures to satisfy requirements such as providing a consumer health data privacy policy, obtaining consumers' consent to collect and share their consumer health data, and providing several consumer rights, among other obligations. Similar requirements regarding consumer health information recently went into effect in Connecticut by virtue of an amendment to the Connecticut comprehensive privacy law (described further here).

Separately, California's SB 345, effective since the start of the year, amended the California Business and Professions Code to ban the collection, use, or disclosure of the personal information of individuals who are physically located at family planning centers, except as necessary for the company to provide services requested by the individuals.

Other states have also set their sights on protecting sensitive data by enacting or amending laws. For instance, Colorado recently amended the definition of "sensitive data" in its comprehensive privacy law to include a new subcategory, "biological data," which includes the newly defined term "neural data." This expansion aims to address growing concerns over the capabilities of both invasive and noninvasive neurotechnologies to process information about the structure and functioning of individual brains and nervous systems and the use of that information to identify individuals.

Federal regulators — in particular the Federal Trade Commission (FTC) — also continue to prioritize health and other sensitive information generally. For instance, the FTC recently entered into a settlement with X-Mode Social and its successor Outlogic (X-Mode), after the data broker allegedly sold precise location data that could be used to track visits to sensitive locations such as medical and reproductive health clinics, places of religious worship, and domestic abuse shelters. In addition to banning X-Mode from sharing or selling precise location data, the consent order requires X-Mode to destroy all location data previously collected and any products developed from this data, and significantly strengthen its privacy compliance measures, including by establishing and implementing a comprehensive privacy compliance program.

Together, these state laws and regulatory enforcement activity evidence an increased focus on sensitive and health data privacy, imposing new obligations and reshaping the regulatory landscape for this information across industries. Compounding the regulatory risk, businesses subject to MHMD also face a new threat of civil litigation, as the statute provides Washington consumers with a private right of action to enforce their rights.

New State Youth Privacy Laws

Turning to another category of heightened privacy regulation taking hold this year, several new state laws aim to enhance the protection of minors' online privacy and safety. As noted below, district courts have already enjoined a number of these laws in courts, making their future uncertain. Many of these laws impose new parental consent requirements for minors to use online services (and Florida prohibits minors under 14 from having accounts at all starting in January 2025) and specific product design obligations, with variance in the age thresholds for what constitutes a minor, including:

- **California:** The California Age-Appropriate Design Code (AB 2273) enforces stricter privacy settings and transparency requirements for businesses offering online services popular with users under 18. This law was set to go into effect on July 1, 2024, but has been enjoined.

- **Utah:** Utah is set to enforce two laws (SB 194 / HB 464) that requires social media platforms to verify the age of account holders, require parental consent for users under 18, ban the serving of ads to minors, and prohibit addictive platform designs.

- **Louisiana:** The Secure Online Child Interaction and Age Limitation Act (SB 162 will require social media platforms to obtain parental consent and/or grant parental access to minors' accounts.

- **Texas:** The Texas Securing Children Online through Parental Empowerment Act, (SCOPE / HB 18) will require social media platforms to obtain parental consent and/or grant parental access to minors' accounts.

- **Florida:** The state's new law on the Protection of Children in Online Spaces (HB 3) will require companies to adopt safer product designs to minimize risks for minors under 18 and ban minors under age 14 from having their own social media accounts.

- **Connecticut:** Amendments to Connecticut's existing comprehensive privacy law (CTDPA / SB 3) will require companies to adopt safer product designs to minimize risks for minors under 18.

- **Ohio:** The Social Media Parental Notification Act (part of HB 33) requires parental consent for minors under 16 to create online accounts and is designed to protect youth mental health from what certain lawmakers deem "intentionally addictive" features. This law was due to take effect in January 2024, but has been enjoined.

- **Mississippi:** The Walker Montgomery Protecting Children Online Act (HB 1126) requires age verification of all users, parental consent for minors under 18, strict data use limitations on minors' data with narrow exceptions, and empowers parents and legal guardians with a private right of action for injunctive / declaratory relief.

These laws face ongoing legal challenges brought under the First Amendment and Due Process Clause, and district courts have preliminarily enjoined the laws in Arkansas (which was due to take effect in September 2023), California, and Ohio. Utah preemptively repealed and replaced its laws in an attempt to avoid a similar injunction; it remains to be seen if this strategy will be successful. As such, the constitutionality and enforceability of this category of laws remains uncertain.

New Online Platform Laws

California and Connecticut also implemented legislation this year aimed at regulating specific online platforms. Like the new state youth privacy laws, some of these laws have been challenged.

California's AB 587 requires social media companies to disclose specific information in their online Terms of Service (TOS) and regularly report to the Attorney General about their TOS and content moderation practices with regard to hate speech and misinformation. Companies that misreport information can face daily fines of $15,000. This law has been challenged in court on free speech grounds, and that challenge has since been denied. Similarly, online platform laws in both Texas and Florida have faced legal challenges, with a decision from the US Supreme Court pending. Additionally, starting January 1, 2024, Connecticut's SB 3 requires online dating platforms to create an online safety center and adopt clear policies to address harassment.

These legislative efforts reflect a broader legislative commitment to heightened Internet safety and transparency standards and require businesses to potentially revamp their practices.

Increased Regulation of Data Brokers

The data broker industry also continues to be a focal point for legislators and regulators alike, which may have ripple effects across the country, not only for data brokers, but also for companies that rely on data brokers. New rules regulating data brokers went into effect in Texas (September 1, 2023) and Oregon (January 1, 2024) and between 2024 to 2028, different provisions of the California Delete Act (SB 362) —

which amends California's existing Data Broker Registration law — will go into effect and impose new requirements on data brokers, including that they must:

- provide more detailed information in their annual registrations and privacy policies, including whether they collect precise geolocation and metrics relating to their processing of consumer rights requests brought under the California Consumer Privacy Act (CCPA) during the prior calendar year;
- utilize California's new statewide deletion mechanism to process requests to delete personal information; and
- allow for independent, third-party audits every three years to confirm they are following the new law.

In light of the FTC's early 2024 enforcement activity against data brokers and a general increase in scrutiny on the industry, businesses that may qualify as data brokers under the California Delete Act and companies that obtain information from such data brokers should pay careful attention to the law's effective dates and obligations.

Additional Changes in California

Finally, beyond the specific areas discussed above, California continues to take steps to enhance privacy regulation across the board, including by enacting new legislation and rules. For example, the CCPA was updated this year to include "citizenship and immigration status" within the definition of "sensitive personal information." Moreover, pursuant to the CCPA, the California Privacy Protection Agency (CPPA) Board recently voted to prepare new regulations on risk assessments, automated decision-making technology, and cybersecurity audits (as well as updates to existing regulations) for formal rulemaking, a process that will likely commence in summer 2024, with the goal of adopting the new regulations in 2025.

The California legislature also introduced a bill this year (AB 3048) that would require businesses that develop or maintain a browser or device through which consumers interact with a business to include a setting that enables the consumer to send an opt-out preference signal. This bill provides the CPPA with broad authority to adopt regulations as necessary to implement and administer the bill.

Conclusion

As we look ahead to the remainder of 2024 and beyond, it is clear that the patchwork of US state privacy laws will continue to expand and evolve, demanding vigilance and adaptability from affected businesses. Businesses must not only prepare for the immediate impact of these laws, but also stay informed about potential future legislation. Proactive measures — such as understanding the information a business collects and how it is used and disclosed, conducting regular reviews of privacy notices and policies, investing in strengthening privacy compliance measures, and training employees on compliance best practices — will be key to navigating this increasingly complex regulatory environment.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Michael H. Rubin
michael.rubin@lw.com
+1.415.395.8154
San Francisco

Robert W. Brown
robert.brown@lw.com
+1.713.546.7454
Houston / Austin

Max G. Mazzelli
max.mazzelli@lw.com
+1.415.395.8040
San Francisco

Jennifer Howes
jennifer.howes@lw.com
+1.415.395.8815
San Diego / San Francisco

Sarah Zahedi
sarah.zahedi@lw.com
+1.415.395.8069
San Francisco

You Might Also Be Interested In

FTC Proposes Updates to COPPA Rule

FCC Expands Data Breach Notification Rules

Oregon and Delaware Join the Surge of US States Enacting General Privacy Legislation

Recently Enacted Health Data Privacy Laws in Washington and Nevada Pose Challenges for Businesses

Connecticut Passes Significant Amendments to the Connecticut Data Privacy Act

Florida Digital Bill of Rights Adds to the Growing US State Privacy Network